REMARKS

Claims 1-4, 6, 8-21, 23, 25-38, 40, and 42-51 were pending. Claim 1 has been amended to more closely parallel claims 18 and 35. Claim 18 has been amended to correct a typographical error. Accordingly claims 1-4, 6, 8-21, 23, 25-38, 40, and 42-51 remain pending in the application.

35 U.S.C. § 102(e) Rejections

In the present Office Action, claims 1-2, 6, 8, 10, 12, 15-16, 18-19, 23, 25, 27, 29, 32-33, 35-36, 40, 42, 44, 46, and 49-50 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Bots, U.S. Patent No. 6,226,748 (hereinafter "Bots"). Applicant submits that the claims recite features and limitations not suggested or taught by the cited art. Applicant respectfully traverses the above rejections and requests reconsideration in view of the following discussion.

In the present Office Action, on page 2, line 29 to page3, line 18, it is suggested that Bots discloses all of the features of claims 1, 18, and 35. For example, it is suggested

"the applicant discloses a method of controlling information flow through a firewall comprising the following limitations which are met by Bots:
a) determining a first incoming packet community set (PCS) of a first data packet received on an interface of said firewall (Col. 7, lines 1-6);
b) discarding said first data packet in response to detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface (Col. 8, lines 2-4);
processing said first data packet in response to detecting said first incoming PCS is a subset of said IFCS, wherein said processing comprises:
c) matching said first data packet to a first rule of a plurality of rules of said firewall (Col. 7, lines 1-19);
d) comparing said first incoming PCS to a second incoming PCS specified by the first rule (Col. 7, lines 1-19);
e) changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS (Col. 7, lines 1-19);

f) comparing said outgoing PCS with a destination community set of said first data packet, prior to transmitting the first data packet to said destination community (Col. 7, line 56 to Col. 8, line 14; Fig. 4);

g) discarding said first data packet in response to detecting said outgoing PCS is not a subset of said destination community set (Col. 8, lines 2-4);

h) further processing said first data packet in response to detecting said outgoing PCS is a subset of said destination community set (Col. 7, line 56 to Col. 8, line 14; Fig. 4)."

Also, on page 7 line 25 to page 8, line 6 the Examiner asserts:

"Bots discloses a method of controlling information flow. Referring to Fig. 2, an end station (e.g. 211, 212, 213) may want to transfer a data packet to a destination (e.g. 201, 202,203). VPN Units (252, 250) control information flow. Specifically, a data packet from an end station (211,212,213) may pass through a first VPN Unit (e.g. 252) where it is processed (Col 7, lines 45-52). After the packet is processed it is forwarded toward the destination address over the Internet (Col. 7, lines 52-55).

Before the packet is delivered to its destination, it may be processed again at a second VPN Unit (e.g. 250) (Col. 7, line 56 to Col. 8, line 14). At the second VPN Unit, the outgoing PCS of the packet is compared with a destination community set. Finally, the packet at the second VPN Unit will either be sent to the destination community (Col. 8, lines 12-14) or discarded."

However, claim 35 reads as follows:

"A computer network comprising:
a node configured to act as a firewall, wherein said node comprises:
a processing unit, wherein said processing unit is configured to:
  determine a first incoming packet community set (PCS) of a first
    data packet received on an interface of said node;
  discard said first data packet in response to detecting said first
    incoming PCS is not a subset of an interface community set
    (IFCS) of said interface; and
  process said first data packet in response to detecting said first
    incoming PCS is a subset of said IFCS, wherein processing
    the first data packet comprises:
    matching said first data packet to a first rule of a plurality
      of rules of said firewall;
    comparing said first incoming PCS to a second incoming
      PCS specified by the first rule; and
    changing the first incoming PCS in the first data packet to
      an outgoing PCS specified by the first rule, in

response to determining the first incoming PCS
matches the second incoming PCS;
comparing said outgoing PCS with a destination
community set of said first data packet, prior to
transmitting the first data packet to said destination
community;
discarding said first data packet in response to detecting
said outgoing PCS is not a subset of said destination
community set; and
further processing said first data packet in response to
detecting said outgoing PCS is a subset of said
destination community set; and
a community information base coupled to said processing unit;
a first computer network coupled to said node; and
a second computer network coupled to said node."

Applicant submits that claim 35 recites features not disclosed by Bots. Generally speaking, claim 35 recites multiple steps performed by a processing unit within "a node configured to act as a firewall." It is noted that a single processing unit is configured to determine, discard, and process the first data packet within a single node. It appears from the assertions above that the Examiner generally cites a pair of Bots's VPN Units (e.g. 250 and 252) controlling information flow. However, Bots clearly shows in Fig. 2, that VPNUs, such as VPNU 250 and VPNU 252, are separate nodes interconnected through the "Internet/Public or Unsecure Network Space". The methods taught by Bots which are said to disclose the features of claim 35 are not performed within a single node. Moreover, Bots's interconnection through the unsecure network exposes information in a way that is not consistent with the function of a firewall. For at least the above reasons, Applicant submits that Bots fails to teach all of the features of claim 35.

For at least the above reasons, Applicant submits that claim 35 is patentably distinguishable over the cited art. Further, as each of independent claims 1, as amended, and 18 include similar features, each of claims 1 and 18 are believed patentable for similar reasons. Likewise, each of the dependent claims 2-4, 6, 8-17, 19-21, 23, 25-34, 36-38, 40, and 42-51 include at least the features of the independent claims upon which they depend, each of the dependent claims are patentable as well.

Also, even if for the sake of argument it is assumed that a pair of VPNUs is equivalent to a node configured to act as a firewall, Bots fails to disclose all of the features of claims 1, 18, and 35. For example, claim 1 recites, in relevant part:

> "... matching said first data packet to a first rule of a plurality of rules of said firewall;
> comparing said first incoming PCS to a second incoming PCS specified by the first rule;
> changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS ..."

Applicant submits that Bots fails to disclose "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule, in response to determining the first incoming PCS matches the second incoming PCS", as is recited in claim 1. Bots does disclose:

> "The particular packet processing algorithms to be used for VPN traffic may vary, so long as the lookup tables in both the sending and receiving VPN units identify the same compression, encryption and authentication rules and are capable of implementing and deimplementing them for members of the same group. It is to be understood that a single VPNU may serve multiple VPN groups and that particular addresses may be members of multiple groups. Thus, at step 340, when a packet is destined from one member of the VPN group to another, the packet is processed according to the compression, encryption and authentication rules identified in the VPNU tables for that particular VPN group." (Bots, Col. 7, lines 40-52).

While Bots discloses processing steps of compression, encryption, and authentication, Bots fails to teach or suggest changing the VPN group. Compression, encryption, and authentication are well-known processes that do not change group membership. Accordingly, Applicant submits that Bots fails to teach "changing the first incoming PCS in the first data packet to an outgoing PCS specified by the first rule," as is recited in claim 1.

In addition, claim 1 recites three comparisons: detecting said first incoming PCS is not a subset of an interface community set (IFCS) of said interface, comparing said first incoming PCS to a second incoming PCS specified by the first rule, and comparing said outgoing PCS with a destination community set of said first data packet. Bots fails to teach or suggest all three comparisons. In contrast to the above claimed features, Bots discloses:

> "At decision box 320, it is determined whether or not the source and destination addresses for the data packet are both members of the same VPN group. This determination may be made with reference to lookup tables that are maintained by the VPN units or reference to other memory mechanisms. This step may be thought of as member filtering for data packets being transmitted between the particular site and the VPN unit which services it." (Bots, Col. 7, lines 1-9).

> "At decision box 420, the inbound data packet is examined to determine if the source and destination addresses of the data packet are both members of the same VPN group. It is assumed that the lookup tables maintained by all of the VPN units are both consistent and coherent." (Bots, Col. 7, lines 60-65).

As may be seen from the above, Bots's method looks up the VPN group of the source address and the VPN group of the destination address and compares them to see if the two groups are the same. These steps are performed in both the transmitting VPNU and the receiving VPNU. Hence, Bots discloses, at most, two comparisons. Furthermore, since Bots does not disclose changing the source or destination address between the first VPNU and the second VPNU, and since Bots assumes that the lookup tables maintained by all of the VPN units are both consistent and coherent, Bots's second comparison is a repetition of the first comparison, i.e. it is a comparison of the source VPN group with the destination VPN group. In contrast, the three comparisons recited in claim 1 involve a first incoming PCS and an (IFCS), a first incoming PCS and a second incoming PCS, and an outgoing PCS and a destination community set. No two of these comparisons involve the same two community sets. Accordingly, Applicant submits that Bots fails to disclose more than one of the comparisons recited in claim 1.

Also, there are significant additional differences between the comparisons disclosed by Bots and the claimed features. For example, Bots compares the VPN group of the source address with the VPN group of the destination addresses to see if they are the same. However, Bots does not disclose detecting if any group is a subset of any other group. Accordingly, Bots neither teaches nor suggests "discarding said first data packet in response to detecting said first incoming PCS **is not a subset of an interface community set (IFCS)** of said interface" or "discarding said first data packet in response to detecting said outgoing PCS **is not a subset of said destination community set**," as is recited in claim 1.

Further, on page 6, lines 7-18 of the present Office Action, the Examiner asserts:

"As per claims 4, 13, 21, 30, 38, and 47, the applicant discloses the method of claims 1, 12, 18, 29, 35, and 46, which are met by Bots, with the following limitation which is net by Kidambi:
Wherein said incoming PCS is encoded in a header of said first data packet, and wherein said determining comprises decoding said incoming PCS from said header of said first data packet (Kidambi: Col 25, line 53 to Col 26, line 3 and Bots: Fig 6);
Bots discloses all the limitations of the claim except for the limitation that the source and destination addresses are decoded from the header. Kidambi discloses the idea of encoding the source and destination addresses in the header. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to encode the source and destination addresses on the header of a data packet because doing so is a commonly accepted method of effectively transmitting the source and destination addresses."

It would appear from the above that the Examiner is generally identifying the source and destination addresses of either Kidambi or Bots as being equivalent to the claimed PCS. Applicant respectfully submits that the PCS refers to something broader than the source and destination addresses. Page 11 of the Specification recites

"Determine the Packet Community Set (PCS) of the packet from the intersection of the source NACS and the destination NACS."

and

"In the embodiment shown in Figure 1, two associations are maintained in the CIB: (1) for each node in the enterprise network (identified by the node's network address), the user community or set of communities which the node serves, and (2) for each network interface on the MCN, the user community or set of communities associated with the network attached to the network interface. Association 1 may be referred to as the Network Address Community Set (NACS)."

Thus, the PCS is the intersection of the user community or set of communities which the source node serves and the user community or set of communities which the destination node serves. Clearly, the user community that the source node serves may include more than the source address. The same is true for the destination node. Accordingly, Applicant submits that Bots teaching of the source and destination addresses is not equivalent to the claimed PCS.

For at least the above additional reasons, Applicant submits that claim 1 is patentably distinguishable over the cited art. Further, as each of independent claims 18 and 35 include similar features, each of claims 18 and 35 are believed patentable for similar reasons. Likewise, each of the dependent claims 2-4, 6, 8-17, 19-21, 23, 25-34, 36-38, 40, and 42-51 include at least the features of the independent claims upon which they depend, each of the dependent claims are patentable as well.

In addition, claims 3, 11, 20, 28, 37, and 45 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of McNeill, U.S. Patent No. 6,167,052. Claims 4, 13, 21, 30, 38, and 47 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of Kidambi, U.S. Patent No. 6,424,626. Finally, claims 14, 17, 31, 34, 48, and 51 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Bots in view of Kisor, U.S. Patent No. 6,266,773. As each of the dependent claims include at least the features of the independent claims upon which they depend, each of the dependent claims are patentable for at least the above reasons. No further discussion of the dependent claims is believed necessary at this time.

Applicant believes the application to be in condition for allowance. However, should the examiner believe otherwise, the below signed representative requests a telephone interview (512) 853-8866 in order to facilitate a speedy resolution.
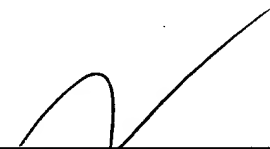
CONCLUSION

Applicant submits the application is in condition for allowance, and an early notice to that effect is requested.

If any extensions of time (under 37 C.F.R. § 1.136) are necessary to prevent the above referenced application(s) from becoming abandoned, Applicant(s) hereby petition for such extensions. If any fees are due, the Commissioner is authorized to charge said fees to Meyertons, Hood, Kivlin, Kowert, & Goetzel, P.C. Deposit Account No. 501505/5181-75900/RDR.

Also enclosed herewith are the following items:

☒ Return Receipt Postcard

Respectfully submitted,

Rory D. Rankin
Reg. No. 47,884
ATTORNEY FOR APPLICANT(S)

Meyertons, Hood, Kivlin,
   Kowert, & Goetzel, P.C.
P.O. Box 398
Austin, TX 78767-0398
Phone: (512) 853-8800

Date: June 2, 2006